CLAIMS

1. A computer implemented method for preventing malicious code from propagating in a computer, the method comprising the steps of:

a blocking-scanning manager detecting attempted malicious behavior of running code;

responsive to the detection, the blocking-scanning manager blocking the attempted malicious behavior;

the blocking-scanning manager generating a signature to identify the code that attempted the malicious behavior;

the blocking-scanning manager detecting code identified by the signature; and

the blocking-scanning manager blocking the execution of the identified code.

2. The method of claim 1 wherein a source of at least one of the running code and the identified code comprises a source from a group of sources consisting of an e-mail attachment, a magnetic medium, an optical medium, a file, a boot sector, and a network remote computer.

3. The method of claim 1 wherein the blocking-scanning manager detecting code identified by the signature further comprises the blocking-scanning manager comparing the running code to at least one signature generated.

4. The method of claim 3, wherein the blocking-scanning manager comparing the running code to at least one signature generated further comprises the blocking-scanning manager determining that the running code matches at least one of the generated signatures.

5. The method of claim 1 wherein the blocking-scanning manager detecting code identified by the signature further comprises the blocking-scanning manager placing at least one of the running code and the identified code in a repository, such that the user cannot execute the code.

6. The method of claim 1 further comprising:

the blocking-scanning manager performing the detecting step on a first computer able to connect to a network;

the blocking-scanning manager placing at least one of the running code and the identified code in a repository located at a location from a group

consisting of locally on the first computer, and remotely on a second computer able to connect to the network; and

the blocking-scanning manager performing the blocking step at a location from a group consisting of locally on the first computer or remotely on a second computer able to connect to the network.

7. The method of claim 1 wherein detecting code identified by the signature further comprises:

the blocking-scanning manager alerting a user of the detection; and

the blocking-scanning manager allowing the user to choose whether or not to block the execution of the identified code.

8. The method of claim 7 further comprising the blocking-scanning manager overriding the user's choice responsive to the user incorrectly choosing to block non-malicious behavior or incorrectly choosing not to block malicious behavior.

9. The method of claim 1 further comprising the blocking-scanning manager regulating the number of signatures generated within a period of time.

10. The method of claim 9 wherein regulating the number of signatures further comprises:

the blocking-scanning manager recognizing a predetermined limit on the number of signatures generated within a period of time;

responsive to reaching the predetermined limit, the blocking-scanning manager removing older signatures as newer signatures are generated

11. The method of claim 9 wherein regulating the number of signatures further comprises:

the blocking-scanning manager sorting the signatures according to number of matches per signature to running code that attempted malicious behavior; and

responsive to reaching the predetermined limit, the blocking-scanning manager removing the signatures with the fewest matches as newer signatures are generated.

12. The method of claim 1 wherein the blocking-scanning manager blocking the execution of the identified code further comprises the blocking-scanning manager associating a name with the identified code.

13. The method of claim 12 wherein associating a name with the identified code further comprises the blocking-scanning manager changing the name to accord with a new definition of the identified code in a database of known malicious code.

14. The method of claim 1 wherein the blocking-scanning manager generating a signature to identify the code that attempted the malicious behavior further comprises:

the blocking-scanning manager applying a checksum function to generate a checksum of the code that attempted the malicious behavior;

the blocking-scanning manager storing the checksum; and

the blocking-scanning manager using at least one stored checksum to identify code that attempted malicious behavior.

15. The method of claim 1 wherein the blocking-scanning manager generating a signature to identify the code that attempted the malicious behavior further comprises:

the blocking-scanning manager applying a hash function to generate a hash of the code that attempted the malicious behavior;

the blocking-scanning manager storing the hash; and

the blocking-scanning manager using at least one stored hash to identify code that attempted malicious behavior.

16. The method of claim 15 wherein the blocking-scanning manager applying a hash function to generate a hash further comprises the blocking-scanning manager generating a hash of at least a portion of a code segment of computer-readable contents associated with the code.

17. The method of claim 15 wherein the blocking--scanning manager applying a hash function to generate a hash further comprises the blocking-scanning manager generating a hash of at least a portion of a data segment of computer-readable contents associated with the code.

18. The method of claim 15 wherein the blocking-scanning manager applying a hash function to generate a hash further comprises the blocking-scanning manager generating a hash of at least a portion of a header of computer-readable contents associated with the code.

19. A computer system for preventing the propagation of malicious code, the computer system comprising:

a running code detection module, configured to detect attempted malicious behavior of running code;

a running code blocking module, configured to block the attempted malicious behavior in response to positive detection, the running code blocking module being communicatively coupled to the running code detection module;

a signature module, configured to generate a signature to identify the code that attempted the malicious behavior, the signature module being communicatively coupled to the running code blocking module;

an scanning module, configured to detect code identified by the signature, the scanning module being communicatively coupled to the signature module; and

an identified code blocking module, configured to block the execution of the identified code, the identified code blocking module being

communicatively coupled to the scanning module.

20. The computer system of claim 19, further comprising a repository, configured to store at least one of the running code and the identified code, such that the user cannot execute the code, the repository being communicatively coupled to the running code detection module and the scanning module.

21. The computer system of claim 19, wherein the scanning module is further configured to compare running code to at least one signature generated, the scanning module being communicatively coupled to the signature module.

22. The computer system of claim 19, further comprising an alert module, configured to alert a user of detection of attempted malicious behavior of code, wherein the alert module is further configured to allow a user to choose whether or not to block the execution of the code, the alert module being communicatively coupled to the running code detection module and the scanning module.

23. The computer system of claim 22, wherein the alert module is further configured to override the user's choice responsive to the user incorrectly choosing to block non-malicious behavior or incorrectly choosing not to block malicious behavior.

24. The computer system of claim 19, further comprising a signature regulation module, configured to regulate the number of signatures generated within a period of time, the signature regulation module being communicatively coupled to the signature module.

25. A computer-readable medium containing a computer program product for preventing the propagation of malicious code in a computer, the computer program product comprising:

program code for a blocking-scanning manager detecting an attempted malicious behavior of a running code;

program code for the blocking-scanning manager blocking the attempted malicious behavior in response to the detection;

program code for the blocking-scanning manager generating a signature to identify the code that attempted the malicious behavior;

program code for the blocking-scanning manager detecting code identified by the signature; and

program code for the blocking-scanning manager blocking the execution of the identified code.

26. The computer program product of claim 25, further comprising program code for the blocking-scanning manager comparing the running code to at least one signature generated.

27. The computer program product of claim 25, further comprising program code for the blocking-scanning manager associating a name with the identified code.

28. The computer program product of claim 25, further comprising:

program code for a blocking-scanning manager alerting a user of detection of attempted malicious behavior of code; and

program code for a blocking-scanning manager allowing a user to choose whether or not to block the execution of the code.

29. The computer program product of claim 28, further comprising program code for a blocking-scanning manager overriding the user's choice responsive to the user incorrectly choosing to block non-malicious behavior or incorrectly choosing not to block malicious behavior.